因数分解について(数式処理と数学研究への応用)

AUTHOR(S):

斎藤, 友克; 平野, 照比古

CITATION:

斎藤, 友克 ...[et al]. 因数分解について(数式処理と数学研究への応用). 数理解析研究所講究録 1992, 811: 1-6

ISSUE DATE:

1992-10

URL:

http://hdl.handle.net/2433/83036

数理解析研究所講究録
第811巻 1992年 1-6

因数分解について

斎藤友克 (上智大学)
平野照比古 (神奈川工科大学)

1 序論

Kを任意の体とする。ここで扱う K上に係数を持つ n 変数多項式 $F(x,u,\cdots,v)$ は次の性質を持つとする。

$$F(x,u,\cdots,v)=\sum_{i=0}^{n} f_{n-i}(u,\cdots,v)x^{n-i}$$

とおいたとき (x を主変数)

$$f_n(u,\cdots,v)=1 \qquad (\text{多項式がモニック})$$

となる。さらに、この多項式は

$$F(x,u,\cdots,v) \;=\; F_1\cdots F_r \tag{1}$$

と K上で多項式として因数分解され、各 F_iはそれぞれ

$$F_i=(x-\varphi_{\nu_i})\left(x-\varphi_{\nu_{i+1}}\right)\cdots\left(x-\varphi_{\nu_{i+1}-1}\right),\quad i=1,\cdots,r \tag{2}$$

と K上のべき級数環の上で因数分解されるものとする。ここで各φ_kはすべて相異なる (square-free) ものとする。

例 1

$$F(x,y)=x^4+(y+2)x^3-(y^2-4y+1)x^2-(2y^2-y+2)x-y^3-2y^2.$$

を考える。

$$F(x,0)=x^4+2x^3-x^2-2x=(x-0)(x-1)(x+1)(x+2).$$

を利用して次のような yに関するべき級数を求めることができる。

$$\begin{aligned}
F_1 &= (x-0)-0\cdot y+y^2+y^3+0\cdot y^4+\ldots\\
F_2 &= (x-1)+y-y^2-y^3+0\cdot y^4+\ldots\\
F_3 &= (x+1)+y+y^2+2y^3+5y^4+\ldots\\
F_4 &= (x+2)-y-y^2-2y^3-5y^4+\ldots
\end{aligned}$$

このとき

$$F(x,y) - F_1F_2F_3F_4 = y^5\text{以上の項}$$

となっている。

上の例にみられるような $F(x,0) = 0$ が平方因子を含まない多変数多項式 $F(x,y)$ のときにはべき級数解の係数を下から定めて行くことができる。詳しい算法は [1],[3] 等を参照のこと。

上で得られた解$\varphi_i, (i = 1,2,\cdots,n)$ と多項式 $h_i, (i = 1,2,\cdots,k)$ に対して$\lambda_i, (i = 1,2,\cdots,n)$ を未知数とする次のような連立方程式を考える。

$$\begin{cases} \lambda_1\varphi_1 + \cdots + \lambda_n\varphi_n = h_1 \\ \qquad\qquad \vdots \\ \lambda_1\varphi_1^k + \cdots + \lambda_n\varphi_n^k = h_k \end{cases} \tag{3}$$

解を K の範囲で求めるとすれば次の定理が成立する。[2]

定理 1 $k = n$ でこの連立方程式を考えれば

$$\lambda_{\nu_i} = \lambda_{\nu_i+1} = \cdots = \lambda_{\nu_{i+1}-1} = \lambda^{(i)}$$

であり、

$$h_j = \lambda^{(1)}\left(\varphi_{\nu_1}^j + \cdots + \varphi_{\nu_2-1}^j\right) + \cdots + \lambda^{(r)}\left(\varphi_{\nu_r}^j + \cdots + \varphi_{\nu_{r+1}-1}^j\right)$$

のときに限る。

2 べき級数解を組み合わせて因子を求める方法

ここからは簡単のため二変数多項式 $F(x,y)$ で考えるとする。

(2) で求められたべき級数を用いて $F(x,y)$ の因数分解をする、または既約性の判定をするためにはそれらの内からいくつかを選び、積

$$\prod(x - \varphi_i) \tag{4}$$

を作り、それらが多項式になる組み合わせを探せばよい。しかし、すべての組み合わせを単純に調べるのでは $F(x,y)$ の次数 n が大きくなったときに場合の数が増え過ぎて実用にはならない。そこでなんらかの選ぶ基準を設けて場合の数を減らす工夫が必要である。

定理 1 によれば連立方程式 (3) を利用できる。この方法の初めのアイデアは次のようなものであった。

べき級数解をいくつか選んで (4) のような積を作る。もしこれが元の多項式の因子であれば展開したときの係数は yについてもやはり多項式になる。特に因子の x に関する次数 -1 の係数は

$$-\sum\varphi_i$$

であるから、これは多項式になる。これは (3) に現れる初めの式

$$\lambda_1\varphi_1 + \cdots + \lambda_n\varphi_n = h_1$$

において

$$\lambda_i = 0 \ or \ 1 \tag{5}$$

となるような解を求めるということと同じである。ここで h_1 は多項式であるから、

$$\varphi_i = \sum_{k=0}^{\infty} c_k^{(i)} y^k$$

とおけば十分大きな k に対しては

$$\lambda_1 c_k^{(1)} + \lambda_2 c_k^{(2)} + \cdots + \lambda_n c_k^{(n)} = 0 \tag{6}$$

が成立することになる。ここで条件 (5) を付けたままでこの式を満たすようなものを求めるのではすべての組み合わせを調べることと変わりがない。そこでこの条件を落として、十分大きな k をいくつか選び、λ_i に関する線形方程式を解くことで代用する。方程式の一般解を求めそのパラメーター表示を利用すればべき級数解の組み合わせの総数を減らすことができるのではないか。

一般に線形方程式の一般解を求める手間は変数の数が増えても組み合わせの数のように急激には増加しない。したがって、この方法は効率が上がる可能性がある。効率が上がるためにはこの線形方程式の係数で作られる行列

$$A_\ell = \begin{pmatrix} c_\ell^{(1)} & c_{\ell+1}^{(1)} & c_{\ell+2}^{(1)} & \cdots \\ c_\ell^{(2)} & c_{\ell+1}^{(2)} & c_{\ell+2}^{(2)} & \cdots \\ \vdots & \vdots & \vdots & \cdots \\ c_\ell^{(n)} & c_{\ell+1}^{(n)} & c_{\ell+2}^{(n)} & \cdots \end{pmatrix} \tag{7}$$

の階数 (rank) が大きいことが重要である。大きければ自由に動くことのできる変数が少なくなり効率がよい。以上の考察により次のような変形した行列の rank が必要となる。

$$\lim_{\ell\to\infty} \mathrm{rank} A_\ell$$

これは (6) は k が小さいときには成立しないことによる。これを $\varphi_1(y), \ldots, \varphi_n(y)$ の s-rank と呼ぶことにする。ここで ℓ が大きくなるにつれて $\mathrm{rank}A_\ell$ は単調に減少するので極限値は存在する。

(注意) ここでは与えられた多項式が二変数の場合にしか s-rank を定義していないが、一般の場合には全次数で極限をとれば同様に定義される。また、現れる行列の成分は $u^i \cdots v^j$ の係数を並べて作ればよい。

3 s-rank が 1 の場合

多項式の因子が一つあればそれによってそれらの因子に対応するλ_i を 1 にして残りを 0 とする方程式 (6) の解が存在するので s-rank は多項式の因数の数が多ければあまり大きくならないことは明らかである。しがし、そのとき以外にも s-rank が大きくならない場合がある。

例 2 $f(x,y)=x^m-(y+1)^n$とすれば

$$x=\zeta(1+y)^{n/m} \quad (\zeta\text{は 1 の } m \text{ 乗根})$$

であるからこれらの解で張られる線形空間の次元は 1 である。したがって、*s-rank* も 1 である。

この論文の目的は s-rank が 1 になる場合の多項式を確定することである。まず、既約の場合から調べる。

Lemma 1 与えられた多項式

$$F(x,y)=\sum_{i=0}^{n} f_i(y)x^{n-i}$$

が既約であり、$F(x,y)=0$ の根$\varphi_1(y),\cdots,\varphi_n(y)$ の *s-rank* が 1 であるとする。このとき Kの標数が 0 であるか、n を割らないとき

$$g(y)=-\frac{f_1(y)}{n}$$

とおくと、i に無関係なべき級数$\varphi(y)$ と定数 c_1が存在して

$$\varphi_l(y)=g(y)+c_l\varphi(y)$$

と表せる。

[証明] $\varphi_1(y),\ldots,\varphi_n(y)$ の s-rank が 1 であるから

$$\varphi_i(y)=g_i(y)+c_i\varphi_1(y)$$

となる yの多項式 $g(y)$ と Kの定数 c_iが存在する。ここで $c_i\neq 0$ としてよい。(べき級数解は Kで求められるという仮定した。) もし、$c_i=0$ であれば$\varphi_i(y)$ =多項式となり、与えられた多項式が既約であることから $n=1$ となり明らかに定理は成立している。$n>1$ とする。

ここで方程式式 $F(g_i(y)+c_ix,y)=0$ を考えるとこれは $x=\varphi_1(y)$ を根に持つ。

$$\begin{aligned} F(q_i(y)+c_ix,y) &= (c_ix+q_i(y))^n+f_1(y)(c_ix+q_i(y))^{n-1}+\cdots \\ &= c_i^nx^n+c_i^{n-1}(nq_i(y)+f_1(y))x^{n-1}+\cdots \end{aligned}$$

となる。$F(x,y)$ が既約であるからこれは $c_i^n F(x,y)$ に等しくなる。特に、$n-1$ 次の係数を比較して次の式を得る。

$$c_i^n f_1(y) = c_i^{n-1}(ng_i(y) + f_1(y))$$

ここで、Kの標数が n を割らないので

$$g_i(y) = \frac{1}{n}(c_i - 1)f_1(y)$$

である。$g(y) = -\dfrac{f_1(y)}{n}$ とおけば

$$\varphi_i(y) = g(y) + c_i\left(\frac{1}{n}f_1(y) + \varphi_1(y)\right)$$

が得られる。$\varphi(y) = \dfrac{1}{n}f_1(y) + \varphi_1(y)$ とおけばよい。 □

注意 上の証明において $F(x,y)$ の x の関する次数 n が体 Kの標数 p で割り切れる場合は次のようになる。

Kの標数が n を割り切れば $c_i \neq 0$ より

$$c_i f_1(y) = f_1(y)$$

が得られる。つまり $c_i = 1$ または $f_1(y) = 0$ である。$c_i = 0$ であれば

$$\varphi_i(y) = g_i(y) + \varphi_1(y)$$

が得られる。$i \neq 1$ にたいして

$$F(x + g_i(y), y) = 0$$

は $x = \varphi_1(y)$ を解に持つ。$F(x,y)$ と $F(x + g_i(y), y)$ の x^nの係数は共に 1 であるから両者は全く同じ方程式である。つまり、両者の解の集合は一致しなければならない。これより、集合

$$\{g_i(y) | i = 1, \ldots n\}$$

は加法に関して群をなす。この群はガロア体 $GF(p)$ 上のベクトル空間と見なせる。したがって、一次独立なものを選んでその個数を m とすれば集合の要素の数は p^m となる。つまり、$n = p^m$ である。このときはすべての$\varphi_i(x)$ を加えれば 0 になることが分かる。この値は$-f_1(y)$ であるからいずれにせよ $f_1(y) = 0$ が成立する。

この Lemma を用いれば $F(x,y)$ で x の所に $x - \dfrac{f_1(y)}{n}$ を代入することにより $F(x,y)$ の $n-1$ 次の係数を 0 にできる。

Lemma 2 $F(x,y)$ は x に関して n 時で既約であるとする。もし x^{n-1}の係数は 0 で体 K の標数が n を割り切らなければ、$F(x,y)$ の x に関する定数項 $f_n(y)$ は $g(y)^m$ と表すことが出来る。ここに $g(y)$ は適当な多項式である。このとき解$\varphi(y)$ は

$$\varphi(y) = cg(y)^{m/n}$$

と表すことができる。

この Lemma から分かることは s-rank が 1 であるような既約多項式 $F(x,y)$ は円分多項式の変形として得られることである。

3.1 既約でない場合

$F(x,y)=0$ の解の s-rank が 1 であるとする。このとき次の定理が成立する。

定理 2 体 Kの標数は多項式 $F(x,y)$ の x に関する次数 n を割り切らないものとする。この多項式の解の *s-rank* が 1 であれば適当な多項式 $F_0(x,y)$ と yの多項式

$$p_i(y) \quad (i=1,\ldots,m)$$

が存在して

$$F(x,y)=F_0(x+p_1(y),y)F_0(x+p_2(y),y)\cdots F_0(x+p_m(y),y)$$

と表すことができる。

定理は前の Lemma から直ちに得られる。したがって、s-rank が 1 の場合にはいくつかのべき級数解からこれらの因数分解を求めることができる。

4 今後の課題

今後研究すべき課題を挙げる。

1. べき級数はどこまで計算すればよいか。s-rank の決定問題 ([2] に一部検討されている。)
2. s-rank が 1 より大きい場合はどうなるか。
3. 代数閉体まで計算しなくてもべき級数の計算は出来るが、それとの関係はどうなるか。
4. 計算量はどの位か

参考文献

[1] T.Sasaki, M. Suzuki, M. Kolar and M. Sasaki, Approximate Factorization of Multivariate Polynomaial and Absolutel Irreducibility Testing , *to appear*

[2] S. Sasaki, T. Saito, T. Hilano, Analysis of Approximate Factorization Algorithm, I , *submitted*

[3] 平野照比古, 斎藤友克 任意体上の多変数多項式の因数分解, 数式処理通信 Vol.7(1991) No.2 1–5

[4] 佐々木建昭, 佐々木睦子, 多項式因数分解の統一的算法を目指して, 数式処理通信 Vol.7(1991) No.2 6–10